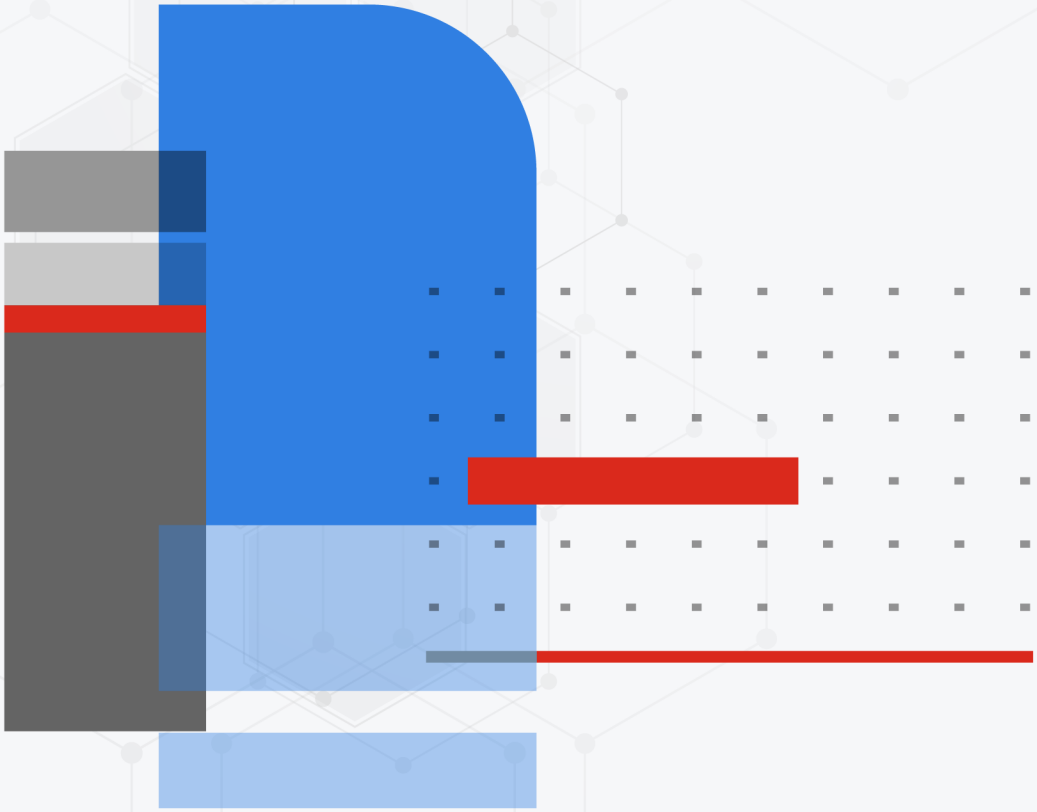
FortiLink Release Notes

FortiSwitchOS 7.4.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

May 15, 2023
FortiSwitchOS 7.4.0 FortiLink Release Notes
11-740-882402-20230515

TABLE OF CONTENTS

Change log

Date	Change Description
May 11, 2023	Initial document release for FortiOS 7.4.0
May 12, 2023	Updated the “What’s new in FortiOS 7.4.0” section.
May 15, 2023	Added bugs 907536, 913718, and 910962.

Introduction

This document provides the following information for FortiSwitch 7.4.0 devices managed by FortiOS 7.4.0 build 2360:

See the Fortinet Document Library for FortiSwitchOS documentation.

Refer to the FortiLink Compatibility table to find which FortiSwitchOS versions support which FortiOS versions.

NOTE: FortiLink is not supported in transparent mode.

The maximum number of supported FortiSwitch units depends on the FortiGate model:

FortiGate Model Range	Number of FortiSwitch Units Supported
FortiGate 40F, FortiGate-VM01	8
FortiGate 6xE, 8xE, 90E, 91E	16
FGR-60F, FG-60F, FGR-60F-3G4G, FG-61F, FG-80F, FG-80FB, FG-80FP, FG-81F, and FG-81FP	24
FortiGate 100D, FortiGate-VM02	24
FortiGate 100E, 100EF, 100F, 101E, 140E, 140E-POE	32
FortiGate 200E, 201E	64
FortiGate 300D to 500D	48
FortiGate 300E to 500E	72
FortiGate 600D to 900D and FortiGate-VM04	64
FortiGate 600E to 900E	96
FortiGate 1000D to 15xxD	128
FortiGate 1100E to 26xxF	196
FortiGate-3xxx and up and FortiGate-VM08 and up	300

New models (NPI releases) might not support FortiLink. Contact Customer Service & Support to check support for FortiLink.

What's new in FortiOS 7.4.0

The following list contains new managed FortiSwitch features added in FortiOS 7.4.0:

- You can now include option-82 data in the DHCP request for DHCP snooping. DHCP option-82 data provides additional security by enabling a controller to act as a DHCP relay agent to prevent DHCP client requests from untrusted sources. You can select a fixed format for the Circuit ID and Remote ID fields or select which values appear in the Circuit ID and Remote ID fields. You can configure the option-82 settings on a global level, or you can override the global option-82 setting to specify plain text strings for the Circuit ID field and the Remote ID field for a specific VLAN on a port. In addition, you can display the DHCP option-82 string in ASCII or hexadecimal format.
- More tests have been added to the FortiSwitch recommendations to help optimize your network:
  - Check if the switch port where a quarantined device was last seen has bouncing enabled.
  - Check if the Basic Input/Output System (BIOS) on the FortiSwitch unit needs to be upgraded before FortiSwitchOS can be upgraded.
  - If the `poe-status` has been enabled under the `config switch-controller auto-config policy` command, FortiOS recommends that you disable it to prevent unpredictable problems caused by connecting two power sourcing equipment (PSE) ports.
- The `execute switch-controller get-conn-status` command now shows when the managed FortiSwitch unit is controlled by VXLAN.
- Two new CLI commands have been added under `config switch-controller system` to improve the FortiLink connection:
  - Use the `set caputp-echo-interval <8-600>` command to set the interval for the Control and Provisioning of Unified Termination Points (CAPUTP) ECHO requests from the Scheduling Wide-area Transport Protocol (SWTP). The default value is 30 seconds. Setting the interval to a shorter time means that an offline device is detected quicker.
  - Use the `set caputp-max-retransmit <0-64>` command to set the maximum number of times that CAPUTP tunnel packets are retransmitted. The default value is 4. Setting the retransmission times to a lower number causes the CAPUTP daemon to time out sooner and then restart for faster failover.
- You can now use the FortiSwitch network access control (NAC) to identify Internet of Things (IoT) and Operational Technology (OT) devices that need to be patched and isolate these devices in a separate VLAN segment. You can specify how severe the IoT and OT vulnerabilities must be for the devices to be isolated.
- You can now use names for managed FortiSwitch units in switch-controller CLI commands. The user-defined name is also used in the FortiOS GUI and logs. The FortiSwitch unit's serial number is saved in a new read-only field.
- You can now use an access control list (ACL) to configure a policy for the ingress stage of the pipeline for incoming traffic. After creating an ACL group for the ingress policy, you apply the ACL group to a managed switch port.

Special notices

Support of FortiLink features

Refer to the FortiSwitchOS feature matrix for details about the FortiLink features supported by each FortiSwitchOS model.

Upgrade information

FortiSwitchOS 7.4.0 supports upgrading from FortiSwitchOS 3.5.0 and later.

To determine a compatible FortiOS version, check the FortiLink Compatibility matrix.

Within the Security Fabric, the FortiSwitch upgrade is done after the FortiGate upgrade. Refer to the latest *FortiOS Release Notes* for the complete Security Fabric upgrade order.

Product integration and support

FortiSwitchOS 7.4.0 support

The following table lists FortiSwitchOS 7.4.0 product integration and support information.

Web browser	• Mozilla Firefox version 52 • Google Chrome version 56 Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS (FortiLink Support)	Refer to the FortiLink Compatibility table to find which FortiSwitchOS versions support which FortiOS versions.

Resolved issues

The following issues have been fixed in FortiOS 7.4.0. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
730472	Initial ARP resolutions are slow when FortiSwitch-enabled VLANs are using access VLANs and proxy ARP.
762615, 765283	The FortiLink flcfg daemon crashes when the configurations pushed to the FortiSwitch unit include the quarantine MAC addresses.
828901	FortiSwitch and FortiAP units are disconnected when the wireless system daemon (hostapd) crashes.
848822	The *Security Rating* page incorrectly lists the version number of the 7.2 FortiAP and FortiSwitch firmware as unknown.
853414	After upgrading from 7.0.5 to 7.0.7, the *Policy* and *Dashboard* widgets do not load when the FortiGate device manages a FortiSwitch unit with tenant ports.
853811	The Link Aggregation Control Protocol (LACP) flaps after the interfaces connecting to LACP are shut down and then restarted from the switch side.
857778	When a VLAN is changed on a FortiGate device, the changes are pushed to the managed FortiSwitch unit but do not take effect.
858113	When the admin profile was created on a FortiGate device, the *Diagnostics and Tools* page for a FortiSwitch unit cannot be displayed with limited access permissions.
858749	Redirected traffic should not hit the firewall policy when `allow-traffic-redirect` is enabled.
859845	Sometimes the correct host names for access points are not displayed in the *FortiSwitch Ports* window.
870083	The FortiGate HA cluster is unsynchronized because of mismatched configurations on the FortiLink interface.
876021	After the FortiGate device is restarted, the FortiLink virtual managed-switch port status is not pushed.
886887	The FortiAnalyzer event log receives too many messages about FortiSwitch MAC entries being discovered.
892576	Previously, the `set rate` command (under `config switch-controller storm-control` and `config switch-controller managed-switch`) could not be set to 0.
894735	Users should be able to use the same EMS tags in multiple NAC policies on different FortiSwitch groups.

Known issues

The following known issues have been identified with FortiOS 7.4.0. For inquiries about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

Bug ID	Description
298348, 298994	Enabling the `hw-switch-ether-filter` command on the FG-92D model (the default setting) causes FortiSwitch devices to not be discovered.
520954	When a “FortiLink mode over a layer-3 network” topology has been configured, the FortiGate GUI does not always display the complete network.
527695	Starting in FortiOS 6.4.0, VLAN optimization is enabled by default (`set vlan-optimization enable` under `config switch-controller global`). On a network running FortiSwitchOS earlier than 6.0.0, this change results in a synchronization error, but the network still functions normally. If you have FortiSwitchOS 6.0.x, you can upgrade to remove the synchronization error or disable VLAN optimization. On a network with `set allowed-vlans-all enable` configured (under `config switch-controller vlan-policy`), the setting reverts to the default, which is disabled, when upgrading to FortiOS 6.4.0. If you want to maintain the allowed-vlans-all behavior, you can restore it after the upgrade.
586801	NetBIOS stops working when proxy ARP is configured and the access VLAN is enabled because FortiGate units do not support NetBIOS proxy.
621785	`user.nac-policy[].switch-scope` might contain a data reference to `switch-controller.managed-switch`. When this reference is set by an admin, the admin needs to remove this reference before deleting the `managed-switch`.
789914	• When LAN segments are enabled on the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, FS-148E-POE, FS-148F, FS-148F-POE, FS-148F-FPOE, FS-124F, FS-124F-POE, and FS-124F-FPOE models, the internal VLAN (`set lan-internal-vlan`) is assigned automatically by default. If the same VLAN is configured on the FortiGate device, the configuration fails when it is pushed to the FortiSwitch unit without any warning message. **WORKAROUND:** Use a custom command. • All sub-VLANs must belong to the same MSTP instance if the FortiLink configuration includes the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, FS-148E-POE, FS-148F, FS-148F-POE, FS-148F-FPOE, FS-124F, FS-124F-POE, and FS-124F-FPOE models.
813216	After CAPWAP offload is enabled or disabled, FortiLink goes down.
814674	When upgrading a FortiAP or FortiSwitch unit that is connected to a downstream FortiGate device, a “Failed to retrieve upgrade progress” message appears.
891642	The FortiGate 6000 and 7000 platforms do not support managing FortiSwitch devices over FortiLink.

Bug ID	Description
905795	After upgrading to FortiOS 7.4, random FortiSwitch units are shown as offline in the GUI when they are actually online. **WORKAROUND:** Deauthorize the FortiSwitch unit and then re-authorize it.
907536	The following FortiSwitch models do not support ACL group 3, which means that they do not support ACL ingress polices: FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-124F, FS-124F-POE, FS-124F-FPOE, FS-148E, FS-148E-POE, FS-148F, FS-148F-POE, FS-148F-FPOE, and FSR-112D-POE.
910962	After setting values for `src-mac`, `dst-mac`, and `vlan` for the ACL classifier, you cannot use the `unset` command to remove these settings. **WORKAROUND:** 1. Remove `set acl-group <ACL_group_name>` from under the `config switch-controller managed-switch` command. 2. Delete the ACL group. 3. Delete the ACL. 4. Reconfigure the ACL.
913718	The FortiLink ACL configuration is not pushed to some of the trunk ports on the FS-548D-FPOE model.

www.fortinet.com